NTM/NJCM-bull. 2017/12

Discussie over gegevensbescherming en de ‘homo digitalis’

Dupliek van Bart van der Sloot

Bart van der Sloot, datum 30-06-2017

Datum	30-06-2017
Auteur	Bart van der Sloot[1]
Folio weergave	Download gedrukte versie (PDF)
Vakgebied(en)	Internationaal publiekrecht / Mensenrechten

In de vorige aflevering van *NTM/NJCM-Bulletin* (jrg. 42, *NTM/NJCM-bull.* 2017/1, p. 3-25) ging Bart van der Sloot onder de titel ‘Het gegevensbeschermingsrecht op de schop: noodzaak of afbraak?’ al in op het pre-advies ‘Homo Digitalis’ dat Lokke Moerel en Corien Prins schreven voor de Nederlandse Juristen Vereniging. In deze aflevering wordt de discussie voortgezet met als voorlopig slotstuk deze dupliek van Bart van der Sloot.

Ik wil Lokke Moerel en Corien Prins danken voor hun uitgebreide reactie. De argumenten zo overziend heb ik het gevoel dat dit pas het begin van een interessante discussie is. Hieronder een aantal vragen die het debat wellicht kunnen voeden.

1) Is Big Data werkelijk zo revolutionair?

De beginvraag is welke impact Big Data, het internet der dingen en de diverse andere technologische ontwikkelingen zullen hebben op ons dagelijks leven. Zoals met alle nieuwe technieken is daar verschil van mening over. Aan de ene kant zijn er indicaties die er op wijzen dat Big Data een revolutie zal ontketenen en ons leven en de maatschappij fundamenteel zal veranderen. Aan de andere kant zijn er ook tekenen dat Big Data in grote mate een hype is en dat veel van de eerste Big Data toepassingen helemaal niet zo effectief zijn gebleken als was voorspeld. Heeft de massale gegevensverzameling door de NSA bijvoorbeeld wel echt de strijd tegen terrorisme bevorderd? Harde bewijzen ontbreken vooralsnog en wellicht zou het geld op een andere manier geïnvesteerd meer resultaten hebben opgeleverd. Moerel en Prins baseren hun pre-advies op de aanname dat Big Data, dat nu nog in de kinderschoenen staat, in de toekomst wel revolutionaire effecten zal hebben, zo revolutionair zelfs dat het gegevensbeschermingsrecht in zijn geheel moet worden herzien. Waarom de argumenten van sceptici volgens hen geen hout snijden wordt echter niet duidelijk, ook niet na lezing van bovenstaande reactie. Dit betekent dat het pre-advies een vermeend gevaar adresseert dat zich in werkelijkheid misschien wel niet of wezenlijk anders zal manifesteren.

2) Waarom zal de Algemene Verordening

Gegevensbescherming geen oplossing bieden?

Er is een evident spanningsveld tussen de wettelijke regels en de praktijk. De regels van dataminimalisatie, doel en doelbinding, datakwaliteit en transparantie die in het huidige gegevensbeschermingsrecht gelden worden op grote schaal genegeerd. De vraag is of de onlangs aangenomen Algemene Verordening Gegevensbescherming, die in mei 2018 EU-wijd van kracht zal gaan, hiervoor een oplossing zal bieden. Ook hieromtrent bestaat geen eenduidig beeld. Een reden om te denken dat de Verordening weinig effect zal sorteren is dat de materiële bepalingen nagenoeg hetzelfde blijven als in de thans geldende Richtlijn Bescherming Persoonsgegevens en de daarop gebaseerde Nederlandse Wet bescherming persoonsgegevens. Aan de andere kant is het zo dat de Verordening directe werking heeft, in samenwerking voorziet tussen verschillende handhavingsorganisaties, deze organisaties significant bredere taken en bevoegdheden toekent en regelt dat er boetes mogen worden opgelegd die kunnen oplopen tot 20 miljoen euro per schending of vier procent van de wereldwijde, jaarlijkse omzet van een bedrijf. Het doel van de Verordening is dan ook om het gat tussen de wet en de praktijk te dichten, maar niet door de wet aan de praktijk aan te passen, zoals in het pre-advies wordt voorgesteld, maar door de praktijk meer in de pas van de wettelijke bepalingen te laten lopen. In het pre-advies wordt uitgegaan van de verwachting dat de Verordening nauwelijks effect zal sorteren, zonder dat deze verwachting nader wordt onderbouwd; ook in bovenstaande reactie geven Moerel en Prins slechts aan ‘te betwijfelen dat de Verordening de beloofde verlossing gaat brengen’. Waarom de Verordening die pas over ruim een jaar in werking treedt al bij voorbaat als kansloos moet worden bestempeld blijft echter in het midden en ook hier worden de argumenten die in een andere richting zouden kunnen niet besproken of weerlegd. Dit betekent dat het pre-advies een oplossing biedt voor een probleem dat mogelijkerwijs reeds door de Algemene Verordening Gegevensbescherming wordt geadresseerd.

3) Waarom volstaan minder radicale voorstellen niet?

In het huidige recht gelden tal van gegevensverwerkingsprincipes, zoals het vereiste van dataminimalisatie, doel en doelbinding, de kwaliteit van persoonsgegevens en het beveiligen van de data. Aan ieder van deze principes moet worden voldaan wil een gegevensverwerkingsproces legitiem zijn. Onder het voorstel van Moerel en Prins worden deze punten niet afzonderlijk behandeld, maar worden zij meegenomen in een algemene belangenafwegingstoets, waarin van geval tot geval de legitimiteit van een gegevensverwerkingsproces wordt beoordeeld door de voor- en nadelen tegen elkaar af te wegen. Niet langer is het dus zo dat als de verantwoordelijke voor de gegevensverwerking de persoonsgegevens niet goed beveiligt, gegevens zonder doel verzamelt of hergebruikt voor nieuwe toepassingen, dit autonomistisch leidt tot een schending van het gegevensbeschermingsrecht – zij ‘zullen in ons voorstel een factor zijn bij de beoordeling van de vraag of sprake is van een gerechtvaardigd belang’.[2] Zijn de baten van een gegevensverwerkingsproces dus hoog genoeg, dan kunnen persoonsgegevens in het voorstel van Moerel en Prins ook zonder legitiem verwerkingsdoel worden verzameld of opgeslagen zonder verdere beveiligingsmaatregelen. Dit staat derhalve diametraal tegenover het huidige gegevensbeschermingsrecht en het pre-advies heeft dan ook zowel binnen de academische wereld als daarbuiten veel stof doen opwaaien. Dat betekent niet dat hun voorstel bij voorbaat moet worden gediskwalificeerd, maar omdat noch uit het pre-advies noch uit bovenstaande

reactie duidelijk wordt waarom minder vergaande oplossingen niet volstaan om het gesignaleerde probleem te adresseren, blijft het onduidelijk of dit verstrekkende voorstel inderdaad noodzakelijk is.

4) Waarom moet het gegevensverwerkingsrecht ook voor ‘small data’ worden herzien?

Het pre-advies beschrijft de ontwikkelingen van Big Data en het internet der dingen en concludeert daaruit dat het huidige gegevensbeschermingsrecht aan verandering toe is. Het pre-advies stelt voor om het gehele gegevensbeschermingsrecht voor alle situaties te herzien. Zelfs als echter wordt aangenomen dat het huidige gegevensbeschermingsrecht inderdaad niet goed werkt ten aanzien van Big Data processen en het internet der dingen, dan nog volgt daaruit slechts dat ten aanzien van déze technieken een alternatief regelgevend kader moet worden gevonden. Niet duidelijk is waarom het dataminimalisatieprincipe, het vereiste dat data moeten worden beveiligd en *up to date* moeten worden gehouden en het uitgangspunt van doel en doelbinding niet zouden werken in de meest voorkomende kleinschalige gegevensbeschermingsprocessen, zoals wanneer een patiënt medische informatie aan zijn dokter geeft. Wordt door Moerel en Prins niet het kind met het badwater weggegooid door het gegevensbeschermingsrecht voor alle situaties te herzien?

5) Is het voorstel wel voldoende kaderstellend voor de private sector?

Het voorstel uit het pre-advies geldt slechts voor de private sector. De auteurs geven aan dat ‘het voorstel dat wij presenteren mogelijk onvoldoende kaderstellend en daarmee beschermend is in de verhouding tussen overheid en burgers’.[3] Als reden geven zij dat de overheid een monopoliepositie heeft en dat overheidsbeslissingen vaak een grotere impact hebben op het leven van burgers. Daarom zou hun voorstel moeten worden aangevuld met strengere regels voor verticale relaties, zo menen zij. Bedrijven als Facebook en Google hebben op bepaalde terreinen echter ook een monopoliepositie en de impact van beslissingen door private partijen als banken, hypotheekverstrekkers en zorgverzekeraars kunnen wel degelijk verstrekkende gevolgen hebben. De vraag die blijft liggen is of er met betrekking tot dergelijke bedrijven met een monopoliepositie en ten aanzien van beslissingen door private partijen met zo’n grote impact op het leven van burgers, ook niet strengere regels van toepassing zouden moeten zijn.

6) Zijn niet alle juridische regels zowel over- als onderinclusief?

Het huidige gegevensbeschermingsrecht is gebaseerd op in de wet vervatte regels en principes. Moerel en Prins wijzen er op dat de gegevensverwerkingsprincipes zowel onder- als overinclusief zijn. Dat wil zeggen, sommige zaken worden door de regels verboden terwijl die eigenlijk prima kunnen worden toegestaan en andere toepassingen slippen door de mazen van de wet en zouden eigenlijk

verboden moeten worden. Als voorbeeld kan worden gegeven hun analyse ten aanzien van het regime voor bijzondere persoonsgegevens, zoals aangaande medische gegevens, geloof en ras. Enerzijds is dit regime volgens de auteurs achterhaald omdat ook uit het gebruik van ongevoelige gegevens, gevoelige patronen of informatie kan worden afgeleid. 'Andersom zijn er genoeg voorbeelden van bijzondere persoonsgegevens die voor het doel waarvoor ze worden verwerkt niet gevoelig zijn, waarmee het onnodig is dat het gebruik aan een zwaarder regime wordt onderworpen. Te denken valt aan het geval dat in de pensioenadministratie iemands partner en geslacht wordt geregistreerd, en daarmee de seksuele geaardheid van de betreffende persoon blijkt.'[4] Het voorstel van Moerel en Prins is dan ook het loslaten van vaste rechtsregels en in plaats daarvan te werken met één open norm, die van geval tot geval moet worden toegepast, zodat de context en de omstandigheden van het geval kunnen worden meegewogen. Daarmee ontstaat volgens hen een granulairder systeem, dat betere en meer specifieke uitkomsten kan bieden dan het huidige rechtsstelsel. Dit is een interessante observatie, die evenwel van toepassing lijkt op vrijwel elke juridische doctrine. De regel dat er zachter moet worden gereden in de bebouwde kom is bijvoorbeeld niet van toepassing op plekken buiten de bebouwde kom waar er onverwachte of gevaarlijke verkeerssituaties kunnen ontstaan en is wel van toepassing op gebieden binnen de bebouwde kom waar er eigenlijk geen reden is tot snelheidsvermindering, bijvoorbeeld op plaatsen waar er bijna nooit mensen de weg oversteken of kinderen spelen. Toch is dit doorgaans geen reden om de rechtsregel als zelfstandig principe op te heffen en onderdeel te maken van een open norm, waarin de bestuurder van verkeerssituatie tot verkeerssituaties moet beoordelen wat een redelijke snelheid is gezien de specifieke omstandigheden van het geval. Niet duidelijk wordt waarom dit voor het gegevensbeschermingsrecht anders zou zijn.

7) Wordt de rechtspositie van de burger daadwerkelijk versterkt?

De vraag is of de burger (het datasubject) inderdaad gebaat is bij een open norm in de vorm van een context-gebonden belangenafwegingtoets. Het voordeel van in de wet vervatte regels en principes is onder meer dat zij een duidelijk normatieve werking hebben en dat ze rechtsgelijkheid en rechtszekerheid bieden. De open norm van Moerel en Prins moet van geval tot geval worden toegepast en zal uitkomsten bieden die context afhankelijk zijn. De vraag is hoe de op de loer liggende rechtsonzekerheid en rechtsongelijkheid in dit systeem kunnen worden vermeden. Onder het huidige gegevensbeschermingsrecht is het onveilig opslaan van gegevens bijvoorbeeld niet toegestaan. Uiteraard bestaat er dan nog discussie over wat precies als veilige gegevensopslag heeft te gelden, maar de vraag of gegevens überhaupt wel veilig moeten worden opslagen, of het dataminimalisatie wel of niet moet worden gevolgd, of het datakwaliteitsprincipe onder bepaalde voorwaarden kan worden ingeperkt, is reeds beantwoord. Als deze rechtsprincipes worden losgelaten en onderdeel worden gemaakt van een algemene belangenafwegingstoets, dan kan een bedrijf bij iedere situatie weer naar voren brengen dat, bijvoorbeeld, de persoons-gegevens weliswaar onveilig waren opgeslagen, maar dat dit geoorloofd was vanwege de hoge baten die er met de gegevensverwerking waren gemoeid. Een rechter zal hier dan een oordeel over moeten vellen, met medeneming van de omstandigheden van het geval. De burger heeft doorgaans echter minder tijd en financiële slagkracht om dergelijke juridische procedures te doorlopen dan de grote data verwerkingsbedrijven als Google en Facebook.

8) Wordt het gegevensbeschermingsrecht inderdaad minder complex voor bedrijven?

Ook is de vraag of bedrijven wel gebaat zijn bij de toepassing van een open norm. In het preadvies wordt gesteld dat de huidige gegevensbeschermingsregels te star zijn en te ver van de huidige praktijk afstaan en zo data-gedreven innovatie belemmeren. Wat daarbij met name als probleem wordt gesignaleerd is dat de huidige gegevensbeschermingsregels te complex zouden zijn voor bedrijven. Het is de vraag of dit inderdaad waar is. Van alle rechtsstelsels lijkt nu juist het gegevensbeschermingsrecht gebaseerd te zijn op vrij voor de hand liggende principes: ‘als u gegevens verwerkt, verzamel dan niet meer dan nodig is’, ‘als u gegevens niet langer nodig heeft, verwijder ze dan’, ‘als u gegevens opslaat, zorg dan dat dit veilig geschiedt’, enzovoorts. Wat het huidige gegevensbeschermingsrecht enigszins ingewikkeld maakt is het feit dat sommige normen interpretatie vergen: wat moet worden gezien als een ‘onverenigbaar doel’, welke technische en organisatorische maatregelen moeten worden getroffen om een afdoende beschermingsniveau te bieden, wanneer zijn data aan te merken als ‘up to date’, enzovoorts. Uiteraard vergen ook in de wet vervatte rechtsregels een soms complex interpretatieproces, maar de oplossing voor het probleem van open principes zoeken in het vervatten van alle zelfstandige rechtsregels in één grote open norm lijkt wat dat betreft het paard achter de wagen spannen.

9) Wie bepaalt de uitkomst van de belangenafwegingstoets en hoe?

In het voorstel uit het pre-advies wordt de uitkomst van de legitimiteitsvraag geboden door een belangenafwegingstoets – de voor- en nadelen van een gegevensverwerkingsproces worden daarin tegen elkaar afgewogen om tot een oordeel te komen. Er is al langer verzet tegen het gebruik van de metafoor van het afwegen van belangen in het recht, omdat belangen geen gewicht hebben en er in de morele en juridische wereld geen weegschaal bestaat om de belangen op een objectieve wijze af te wegen. Dat belangen en de afweging daarvan per definitie een subjectieve interpretatie vergen wordt treffend geïllustreerd in het pre-advies zelf. De auteurs stellen daarin dat het niet als gevoelig valt aan te merken als een persoon werkzaam op de pensioenadministratie iemands partner en geslacht registreert en daarmee de seksuele geaardheid van de betreffende persoon kent. Dit oordeel wordt niet toegelicht en is ook moeilijk objectief te onderbouwen. Dat betekent dat voor iemand anders het subjectieve oordeel anders kan uitvallen, bijvoorbeeld voor de persoon in kwestie. Juist om aan dergelijke subjectieve oordelen te ontkomen werkt het gegevensbeschermingsrecht met regels; gegevens die iemands geaardheid onthullen, hebben nu bijvoorbeeld per definitie als een gevoelig persoonsgegeven te gelden, waarop een apart regime van toepassing is.

10) Is het voorstel wel een oplossing voor het probleem?

Een extra complicerende factor is gelegen in het feit dat het juist bij Big Data initiatieven vaak

uitzonderlijk lastig is om de concrete voor- en nadelen van een gegevensverwerkingsproces te duiden, omdat dit soort processen zich op een tamelijk abstract en algemeen niveau afspelen. Als er miljarden datapunten worden verwerkt en geaggregeerd op een hoog abstractieniveau, zonder dat het daarbij duidelijk is of er persoonsgegevens bij zitten en zo ja, wat de aard daarvan is, en zonder dat het vooraf bekend is met welk concreet doel de gegevens worden verwerkt, dan is het vrijwel ondoenlijk de concrete belangen te duiden die op het spel staan. Biedt het voorstel van Moerel en Prins op dit punt dan ook niet precies de verkeerde oplossing voor het Big Data tijdperk?

11) Wordt met het voorstel het verzamelen van persoonsgegevens vrijgegeven?

Uit het voorgaande volgt ook de vraag wanneer de voorgestane belangenafwegingstoets moet worden toegepast. De huidige gegevensbeschermingsregels gelden met name op het moment dat persoonsgegevens worden verzameld en opgeslagen en bieden zo een barrière tegen ongecontroleerde, onnodige en ondoelmatige gegevensverzamelingen. Op het moment dat gegevens worden verzameld in Big Data processen is vaak echter nog helemaal niet duidelijk welke toepassingen zij precies zullen hebben, noch welke voor- en nadelen daarmee gemoeid zijn. Een dergelijke afweging kan dan ook eigenlijk alleen worden gemaakt op het moment dat de data worden gebruikt, bij de inzet van data-gedreven toepassingen in de praktijk. De auteurs erkennen in het pre-advies dat er in het huidige gegevensbeschermingsrecht tal van barrières gelden voor het verzamelen en analyseren van persoonsgegevens, maar, zo vragen zij zich af, ‘dienen eventuele beperkingen niet veeleer gericht te zijn op de uiteindelijke toepassing van de analyseresultaten? Wij denken dat het laatste het geval is’.[5] Hiermee lijkt het verzamelen van persoonsgegevens dus in feite vrij te worden gegeven en gekozen voor een *use based* benadering van het gegevensbeschermingsrecht.

12) Hoe verhouden de verschillende argumenten zich tot elkaar?

Er wordt in het pre-advies een aantal argumenten gebruikt ter ondersteuning van het voorstel: (i) de huidige regels zijn op zich goed, maar worden verkeerd uitgelegd; (ii) de huidige regels zijn verouderd; (iii) de regels staan te ver van de praktijk; (iv) de regels zijn te complex voor de verantwoordelijke; en (v) de regels zijn te complex voor het individu. In hun pre-advies gaan de auteurs voornamelijk in op het feit dat gegevensbeschermingsregels als het doelbindingsprincipe verouderd zijn. In hun repliek staan de auteurs voornamelijk stil bij de bescherming van de autonomie van het individu. Tussendoor speelt nog een aantal andere argumenten. De vraag is hoe deze argumenten zich tot elkaar verhouden. Als het punt bijvoorbeeld is dat het huidige gegevensbeschermingsrecht op zich goed is, maar in de praktijk te stringent wordt uitgelegd, dan lijkt een heel andere oplossingsrichting voor de hand te liggen dan als het primaire punt is dat deze regels verouderd zijn en niet meer van deze tijd. Gaat het nu om al deze argumenten en zo ja, hoe verhouden die zich dan tot elkaar? Of is er één het hoofdargument en zo ja, welk argument is dat dan?

13) Zijn data inderdaad een doel op zich en kunnen bedrijven niet zonder data?

Daarnaast is het de vraag in hoeverre de inhoudelijk argumenten uit het pre-advies overtuigen. Een voorbeeld is dat in het pre-advies wordt gesteld dat in Big Data processen de data zelf het doel zijn (en dus geen doel meer dienen) en dat daarom het doelbindingsprincipe (dat juist uitgaat van data als middel om een bepaald doel te bereiken) achterhaald is. Echter, ook in Big Data processen dienen data toch een doel? Alhoewel dat doel misschien nog niet direct bekend is of op een hoger abstractieniveau is geformuleerd blijft de doel-middel relatie van data ook bij Big Data bestaan. Het hebben van data zonder daar iets mee te doen is immers voor niemand interessant. Daarnaast stellen de auteurs, met een verwijzing naar Lon Fuller, dat met het huidige gegevensbeschermingsrecht de ‘mogelijkheidszin’ van het recht ondermijnd wordt. Fullers idee van de grenzen van het recht ziet op zaken als het verbieden van homoseksuele handelingen in de privésfeer. De wet kan zijns inziens niet van mensen eisen hun natuur zo te onderdrukken. De vraag die voorligt is in hoeverre dit valt te vergelijken met het gegevensbeschermingsrecht, waarin de grootschalige data-verwerkingsprocessen van internetbedrijven worden ingekaderd door principes als doel en doelbinding, datakwaliteit en veilige opslag. Gaan deze regels zo tegen de ‘natuur’ van internetbedrijven in dat ze de mogelijkheidszin van het recht ondermijnen?

14) Is informed consent wel de hoeksteen van het huidige gegevensbeschermingsrecht?

Moerel en Prins gaan in hun repliek met name in op de informationele zelfbeschikking van het datasubject en het model van *informed consent*. Ze geven aan dat er in Big Data processen simpelweg zoveel gegevens worden verzameld dat het individu niet meer weet wie er allemaal gegevens over hem verzamelen, voor welke doeleinden en aan wie de informatie wordt doorgespeeld. Het is dan ook praktisch ondoenlijk voor het datasubject om zijn individuele rechten en een vorm van persoonlijke controle uit te oefenen, al was het maar vanwege tijdsbelasting in de data-gedreven wereld. Ook in het pre-advies wordt gesteld dat het huidige gegevensbeschermingsrecht op informationele zelfbeschikking is gebaseerd en dat het model van *informed consent* als hoeksteen heeft te gelden. De vraag is of deze aanname klopt. De meeste gegevensverwerkingsprincipes staan juist los van de geïnformeerde toestemming van het datasubject. Persoonsgegevens moeten hoe dan ook goed worden beveiligd; persoonsgegevens moeten altijd correct en *up to date* zijn; als minimumvoorwaarde geldt immer dat persoonsgegevens moeten worden verwijderd als ze niet langer noodzakelijk zijn. Deze principes gelden onder het huidige gegevensbeschermingsrecht ongeacht de vraag of het datasubject toestemming heeft gegeven of niet, ongeacht of hij hierover is geïnformeerd of niet. In het pre-advies wordt in dit verband uitvoerig naar de regels met betrekking tot cookies verwezen, wat de discussie enigszins compliceert. Voor cookies geldt namelijk in tegenstelling tot normale gegevensverwerkingssituaties wel een model van *informed consent*. Dat volgt echter niet uit het gegevensbeschermingsrecht, maar uit het telecommunicatierecht, zoals vervat in het EU Telecommunications Package en de Nederlandse Telecommunicatiewet. De reden om toestemming te vereisen voor het plaatsen van cookies is de bescherming van de integriteit van de computer en

soortgelijke apparatuur van de consument. Externe personen mogen zich niet zomaar toegang verschaffen tot een computer, net zoals ze niet zomaar een woonhuis mogen binnentreden. Daar is toestemming voor nodig. De regels over cookies in de Europese e-Privacyrichtlijn staan dan ook in een bepaling die net zo goed ziet op het plaatsen van *malware* en *spyware* op de computer van een consument. Kortom, het huidige gegevensbeschermingsrecht is maar voor een klein deel gebaseerd op informatierechten en het principe van geïnformeerde toestemming. Het argument dat dit model niet zou werken in de Big Data wereld legitimeert dus slechts op zeer beperkte schaal een herziening van het huidige gegevensbeschermingsrecht. Wat daarbij tevens van belang is dat de auteurs vanuit hun focus op *informed consent* concluderen dat in het huidige gegevensbeschermingsrecht de handhavingsopdracht primair bij individuen ligt (wat huns inziens niet langer werkt, zodat de door hun voorgestane herziening noodzakelijk is). Ook op dit punt is een andere interpretatie van de gegevensbeschermingsregels mogelijk. Zo lijkt de verantwoordelijkheid voor het naleven van de gegevensprincipes primair te liggen bij de organisatie die het doel van de gegevensverzameling bepaalt en de middelen daartoe kiest. Deze (rechts)persoon wordt in het gegevensbeschermingsrecht niet voor niets de 'verantwoordelijke voor de gegevensverwerking' genoemd. Daarnaast ligt de handhavingsopdracht bij de zogenoemde *Data Protection Authorities*, in Nederland de Autoriteit Persoonsgegevens, en kunnen er onder de Algemene Verordening Gegevensbescherming ook *class actions* worden gestart. Het individu speelt dus maar een kleine rol bij de handhaving van het gegevensbeschermingsrecht en deze rol zal met de inwerkingtreding van de Algemene Verordening Gegevensbescherming vermoedelijk alleen maar kleiner worden, onder meer gezien de grote rol voor de *Data Protection Authorities*.

15) Kiezen Moerel en Prins voor een vorm van handeling-utilisme?

Tot slot is de vraag of er zelfs in het voorstel uit het pre-advies geen absolute verboden zouden moeten gelden voor een aantal extreme situaties. In het pre-advies wordt dat expliciet ontkend, in mijn artikel heb ik geprobeerd daarover een debat te ontlokken. 'Neem het lekken van een seksfilm. Dit is onder het huidige recht in principe verboden. Onder de benadering van Moerel en Prins zal van geval tot geval moeten worden bekeken of de voordelen opwegen tegen de nadelen die met de verwerking zijn gemoeid. Als er maar genoeg mensen plezier beleven aan de gelekte sekstape, zullen hun belangen dan opwegen tegen de negatieve effecten op één persoon? Wat als het gezicht van de persoon onherkenbaar wordt gemaakt?'[6] Dit klinkt misschien als een wat sensationeel voorbeeld, maar het dient een doel. De casus is een voorbeeld van een situatie waarbij doorgaans wordt aangenomen dat het lekken van een seksfilm gewoon niet kan, punt uit. Het gaat er dan niet om eventuele voor- en nadelen tegen elkaar af te wegen – dergelijk gedrag is onethisch en zou simpelweg verboden moeten zijn. Dit is een bekende kritiek vanuit de deontologische ethiek – die uitgaat van een aantal handelingen, zoals liegen, stelen en doden, die *an sich* als onethisch worden gezien, ongeacht de eventuele consequenties daarvan – op de ethische stroming die bekendstaat als het consequentionalisme, waarin net als in het voorstel van Moerel en Prins de ethische beoordeling primair wordt bepaald door de mogelijke voor- en nadelen van een handeling tegen elkaar af te wegen. Het voorbeeld van het seksfilmpje heeft dan ook als doel te zoeken naar de vraag of en zo ja waar er in het reguleringsmodel van Moerel en Prins toch reden is om te werken met vaststaande regels en principes, in plaats van met een open belangenafwegingstoets. Daarnaast zou het interessant zijn om hun visie te horen op een

soortgelijke discussie die speelt binnen het consequentionalisme zelf. Moerel en Prins menen dat de vraag of gegevensverwerking geoorloofd is van geval tot geval moet worden beoordeeld. Hiermee lijkt het voorstel in de lijn te liggen van het zogenoemde handelingsutilisme, dat er van uit gaat dat een actie elke keer op zijn eigen merites moet worden beoordeeld. In de literatuur is daar een aantal kanttekeningen bij geplaatst. Om een voorbeeld te geven: het kan best zijn dat in een specifieke situatie de voordelen van een diefstal opwegen tegen de nadelen, bijvoorbeeld omdat de dief erg arm is en de bestolene zo rijk dat die er nauwelijks erg in heeft. Nog los van het deontologische argument dat diefstal simpelweg onethisch is, zijn er ook utilisten die bezwaar maken tegen een dergelijke redenering. Zij wijzen er op dat er hier iets groters op het spel staat, namelijk niet alleen het eigendom van de puissant rijke persoon in kwestie, maar ook het eigendomsrecht als zodanig en het feit dat het van maatschappelijke waarde is om te weten dat eigendom niet zomaar kan worden ontvreemd. Daarom stelt het zogenoemde regel-utilisme voor om niet elke handeling op zijn eigen merites te beoordelen, maar naar de actie als zodanig te kijken: het stelen op zich. In plaats van iedere actie afzonderlijk te beoordelen stelt deze stroming van het consequentionalisme dan ook voor om te werken met vaststaande regels en normen. Misschien toch zo'n gek idee nog niet?

Voetnoten

[1]
Mr. drs. B. van der Sloot is senior researcher aan het Tilburg Institute for Law, Technology, and Society, Universiteit van Tilburg.

[2]
E.M.L. Moerel & J.E.J. Prins, 'Privacy voor de homo digitalis', https://njv.nl/wp-content/uploads/2011/04/Preadviezen-NJV-2016.pdf, p. 13.

[3]
Moerel & Prins (*supra* noot 2), p. 31.

[4]
Moerel & Prins (*supra* noot 2), p. 23-24.

[5]
Moerel & Prins (*supra* noot 2), p. 53-54.

[6]
B. van der Sloot, 'Het gegevensbeschermingsrecht op de schop: noodzaak of afbraak?', *NTM/NJCM-bull.* 2017/1, p. 21.